Upholding information rights

Queen Elizabeth House, Sibbald Walk,
Edinburgh, EH8 8FT
T. 0303 123 1115 E. scotland@ico.org.uk

Minister for Children and Young People
The Scottish Government
St. Andrew's House
Regent Road
Edinburgh
EH1 3DG

By email only

29 January 2021

The Information Commissioner's Office Response to the Consultation on the revised National Guidance for Child Protection in Scotland

The Information Commissioner's Office (ICO) is pleased to respond to the Scottish Government's consultation on the National Guidance for Child Protection in Scotland.

In this submission we have particularly focused on the information sharing aspect of the guidance, however we would be happy to offer more detailed advice on other matters pertaining to data protection if required.

We welcome the inclusion of references to the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018) within the revised guidance reflecting changes in data protection legislation since the original guidance was published 2014. However, we wish to highlight to the Scottish Government that, at the end of the UK's transition period when exiting the EU, the GDPR was incorporated into UK data protection law as the 'UK GDPR' and this sits alongside the DPA 2018. This should be updated within the text of the guidance.

In this submission, we focus on four areas in particular: the first principle of the UK GDPR (lawfulness, fairness and transparency); Privacy by Design and Default; our Data Sharing Code of Practice; and our new detailed right of access guidance.

Lawful, fair and transparent – the first principle

The first principle, set out in Article 5(1) of the UK GDPR states that personal data shall be processed lawfully, fairly and transparently. These three elements work in harmony.

Lawfulness

For the processing of personal data to be lawful, controllers need to identify specific grounds for the processing, also known as a 'lawful basis', from Article 6 of the UK GDPR. The basis may vary for different elements of the child protection process and organisations should consult with their Data Protection Officer to determine which to use and when, and, where appropriate, ensure that relevant data sharing agreements are in place. These lawful bases and any sharing which takes place should be recorded as part of the governance requirements of the UK GDPR.

Our experience shows that practitioners are often unclear about the role of consent when processing personal data. We therefore welcome the section on "Sharing without consent" (p26). In this regard, it should be noted that the UK GDPR sets a high standard for consent and, in most cases where there are child protection concerns, consent is unlikely to be an appropriate lawful basis to rely upon as it requires that individuals have real choice and control about the processing of their personal data. Therefore, if controllers cannot offer a genuine choice – such as when there is a legal duty to process the data - consent would not be appropriate. Nor would it be appropriate if refusal to give consent would prejudice a criminal investigation or might lead to serious harm to the child. Furthermore, due to the power imbalance between a child or families and the authorities, it would be difficult to demonstrate that consent was freely given. In matters of child protection, it is therefore likely that reliance on consent would be the exception and not the rule.

Conditions for processing special category data

The Scottish Government should be aware that there are specific conditions (or legal gateways) in the Data Protection Act 2018 for processing special category data and data relating to criminal convictions and offences (including allegations).

The UK GDPR defines special category data as:

- personal data revealing racial or ethnic origin;
- personal data revealing political opinions;

- personal data revealing religious or philosophical beliefs;
- personal data revealing trade union membership;
- genetic data;
- biometric data (where used for identification purposes);
- data concerning health;
- data concerning a person's sex life; and
- data concerning a person's sexual orientation.

Schedule 1, Part 2, Paragraph 18 of the DPA 2018 provides a specific condition for safeguarding of children and of individuals at risk and sets out when this condition can be relied upon. It may be helpful to highlight this gateway within the guidance and the circumstances it can be relied upon.

Fairness and transparency

Unless a relevant exemption applies (such as doing so would prejudice a criminal investigation), the child should be made aware of the purposes for which their data is being processed and with whom it may be shared. This should be done using age-appropriate language, taking into account the vulnerability of the child.

Relying on a lawful basis other than consent does not prevent agencies or practitioners seeking the child's input or views in relation to their personal data and we are pleased to see this is emphasised within the guidance. This approach would support compliance with the transparency and fairness elements of this principle. These views should be taken into account when making a decision as to whether data should be shared or not and we are pleased to see that this is referenced at multiple points in the guidance.

Data Protection by Design and by Default

The UK GDPR requires organisations to integrate data protection concerns into every aspect of their processing activities, an approach known as 'data protection by design and by default'. It is a key element of the UK GDPR's risk-based approach and its focus on accountability where organisations are obliged to demonstrate how they are complying with data protection requirements.

Organisations engaged in child protection activity should regularly review their processes and procedures to ensure that they are meeting their obligations under both the DPA 2018 and the UK GDPR. Where appropriate, data protection impact

assessments should be undertaken and where high risks to the rights and freedoms of individuals which cannot be mitigated against are identified within the assessment, organisations are required to consult with the ICO under Article 36 of the UK GDPR.

Data Sharing Code of Practice

The ICO has recently published its Data Sharing Code of Practice as guidance and it will be subsequently laid before the UK Parliament prior to it becoming a statutory Code of Practice. It would be helpful if the Scottish Government included a link to this within the guidance so that public authorities or practitioners can seek further information prior to sharing personal data. Public authorities should formalise data sharing agreements for routine data sharing and devise plans that cover ad hoc or emergency data sharing.

Right of access

All data subjects can exercise their right of access to receive copies of their personal information that is held by organisations. This is a qualified right and exemptions exist, for example, where the information may cause serious harm to the individual or disclosure may prejudice the investigation of a crime. More details can be found in our recently published right of access guidance and the Scottish Government may wish to provide a link to this within the child protection guidance.

Finally, the draft National Guidance refers to the development of a National Child Protection Register. At this stage, please note the earlier comments regarding privacy by design and by default and ensure that a data protection impact assessment is undertaken. Also please note that as well as being consulted where high risks to the rights and freedoms of individuals arise and cannot be mitigate against, the ICO must be consulted during the preparation of any legislative instruments relating to the Register. We would therefore welcome being kept informed about the progress of this initiative.

I trust this response is helpful. However, if you would like clarification on any of the points above or advice on any new or emerging data protection issues as this guidance is further developed please do not hesitate to get in touch.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice